

CLAIMS

a 5 1. A method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key (E(NE)) and stored by a recording means ~~(50)~~ on a recording support medium and characterised in that an equivalent of the recording encryption key (E(NE)) is encrypted by a recording transport key (RT(A)) and stored on the support medium together with the encrypted information.

10 2. A method as claimed in claim 1 in which the information encrypted by the recording encryption key (E(NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium.

15 3. A method as claimed in claim 1 ~~or 2~~ in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) are stored on a portable security module ~~(52)~~ associated with the recording means ~~(50)~~.

20 4. A method as claimed in ^{claim 1} ~~any preceding claim~~ in which the transmitted information is encrypted prior to transmission and received by a decoder means ~~(12)~~ before being communicated to the recording means ~~(50)~~.

a a 25 5. A method as claimed in claim 4 in which the decoder ~~(50)~~ is associated with a portable security module ~~(30)~~ used to store transmission access control keys (K0(NS), K0'(Op1,NS) etc.) used to decrypt the transmitted encrypted information.

30 6. A method as claimed in claim 5 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) function in accordance with a second encryption algorithm (CA).

a a 7. A method as claimed in ^{claim 1} ~~any preceding claim~~ in which the recording transport key (RT(A)) is generated at a central recording authorisation unit ~~(21,24,25)~~ and a copy

of this key communicated to the recording means ~~(50)~~.

8. A method as claimed in claim 7 in which the recording transport key (RT(A)) is preferably encrypted by a further encryption key (K0(NSIM)) prior to being communicated to the recording means ~~(50)~~.

9. A method as claimed in ^{claim 1} ~~any preceding claim~~ in which a central access control system ~~(21, 24, 25)~~ communicates transmission access control keys (K0(NS), K0'(Op1, NS) etc.) to the recording means ~~(50)~~.

10. A method as claimed in claim 9 in which the transmission access control keys (K0(NS), K0'(Op1, NS) etc.) are communicated to a portable security module ~~(52)~~ associated with the recording means ~~(50)~~.

11. A method as claimed in claim 9 ~~or 10~~ in which the recording means ~~(50)~~ directly descrambles transmitted information using the transmission access keys (K0(NS), K0'(Op1, NS) etc.) prior to re-encryption of the information by the recording encryption key (E(NE)) and storage on the support medium.

12. A method as claimed in ^{claim 9} ~~any of claims 9, 10 or 11~~ in which the central access control system ~~(21, 24, 25)~~ preferably encrypts the broadcast access control keys (K0(NS), K0'(Op1, NS) etc.) by a further encryption key (K0(NSIM)) prior to their communication to the recording means ~~(50)~~.

13. A method as claimed in ^{claim 9} ~~any of claims 9 to 12~~ in which the recording means ~~(50)~~ sends a request to the central access control system including information identifying the broadcast access keys needed (K0(NS), K0'(Op1, NS) etc.), the request being authenticated by the recording means ~~(50)~~ using a key (K0(NSIM)) unique to that recording means.

14. A method as claimed in claim 1 using a decoder means ~~(12)~~ and associated security module ~~(30)~~ and a recording means ~~(50)~~ and associated security module ~~(52)~~.

a
a

- a

a

20. A method as claimed in claim 19 in which the session key (K3(NSIM)) is generated by the decoder security module or recording means security module (52) and communicated to the other module in encrypted form using an encryption key

(K0(NS)) uniquely decryptable by the other security module.

a
a
a
21. A recording means ~~(50)~~ adapted for use in a method as claimed in ^{claim 1} ~~any preceding claim~~ comprising a security module ~~(52)~~ for encrypting transmitted digital information
5 by a recording encryption key (E(NE)) for storage on a recording support medium and characterised in that the security module ~~(52)~~ is further adapted to encrypt the recording encryption key (E(NE)) by a recording transport key (RT(A)) for storage on the support medium.

a
10 22. A portable security module ~~(52)~~ adapted for use in the recording means of claim 21 and characterised in comprising a recording encryption key (E(NE)) for encryption of transmitted digital information for subsequent recordal and a recording transport key (RT(A)) for encryption of the recording encryption key for subsequent recordal.

a
a
a
15 23. A decoder means ~~(20)~~ adapted for use in a method as claimed in ^{claim 14} ~~any of claims 14 to 20~~ including a security module ~~(30)~~ adapted to store a copy of the recording transport key (RT(A)).

20 24. A decoder means ~~(20)~~ as claimed in claim 23 including a security module ~~(30)~~ adapted to descramble transmitted information using one or more transmission access keys (K0(NS), K0'(Op,NS) etc.) prior to reencryption by a session key (K3(NSIM)) for subsequent communication to a recording means.

a
a
25 25. A portable security module ~~(30)~~ adapted for use in the decoder means ~~(20)~~ of claim 23 ~~or 24~~ and comprising at least a copy of the recording transport key (RT(A)).

26. A method of recording transmitted digital data substantially as herein described.

30 27. A recording means substantially as herein described.

28. A portable security module substantially as herein described.

29. A decoder means ~~substantially as~~ herein described.

001150 22 FEB 90